DRAFT 24 Jan 78/hfm

Threat Study Report

Outline:

Purpose (Objectives of this report; and how one should expect to use the report

Scope (Organization of paper, but also statement of limitations by time available to produce report and availability of information; includes

Definitions (what has been considered as a hostile threat, and who; the totality of the elements of computer security; e.g., people, system, communications, etc.; and any other concepts which should be clearly defined to make the report as meaningful as possible to the reader.)

Statement of the Threat

Analysis of Hostile Potential

Future Change in Threat

Perspective Analysis of Threat (relation between ADP and non-ADP systems)

Conclusions

Recommendations

Appendices (as needed)

~~CONFIDENTIAL~~

D R A F T CONFIDENTIAL 24 Jan 78/hfm

Threat Study Report

Purpose: This report is motivated in part by the DCI's Security Committee's responsibilities for Computer Security as defined in DCID No. 1/11, Amendment 2:

"3. Formulate and recommend to the Director of Central Intelligence resource programming objectives for Intelligence Community organizations in the field of computer security in consideration of current and foreseen vulnerabilities and threats ..."

"4. Coordinate ... Intelligence Community efforts in defense against hostile penetration of Community computer systems ..."

"5. Facilitate within the Intelligence Community the exchange of information relating to computer security threats, ...

"a. The evaluation of foreign intentions and capabilities to exploit Community computer operations;

"b. Central notification of hostile exploitation attempts;

"c. ... damage assessments of incidents of foreign exploitation of intelligence computer operations; ..."

The first issue that needs to be defined for an effective computer security plan is: what is the threat? The threat should serve as a base for what protection is required and what actions are needed to achieve this protection; e.g., R&D, training, awareness, etc. The information provided by this report, then, is intended to serve as:

(1) a base for and justification for allocating Intelligence Community resources to an R&D program for resolving the technical problems associated with the protection of computer operations.

(2) a base for the Intelligence Community to assess system vulnerabilities.

(3) a base for training and indoctrination requirements.

CONFIDENTIAL

(4) an available source of information on foreign intentions, knowledge/capabilities, attempts and successes.

(5) a base for determining effective and efficient use of resources.

Scope: The report presents known and foreseen hostile threats to the protection of intelligence information in ADP systems. It is organized in five major parts as indicated below:

(1) Specific threat cases from sources (incident reports) ((SCOCE, CIA, WWMCCS/CCTC, FBI, Army Report, 1970 Report, etc.))

(2) Analysis of hostile threat potential

- through extrapolation from known cases in (1) above
- defector reports (of interests, motivation, capabilities, etc.)
- information availability in system vs elsewhere, its value, content, significance, etc.
- capability and interest of hostile ((COCOM, TAREX, etc.))
- capability based on domestic crime cases

(3) Hypothesis of future delta (change) in threat based on increased reliance on ADP, internetting, etc.

(4) Relationship of threats in ADP systems to non-ADP world--

- ADP can provide better procedures and structure; i.e., control
- ADP system penetration yields more information, easier, less detectable, less upper management controllability
- Compare where and how information is now captured, relate/translate this to threat impact on ADP world.

(5) Conclusions and Recommendations.